BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 102 17 110.6

Anmeldetag: 17. April 2002

Anmelder/Inhaber: Deutsche Telekom AG, Bonn/DE

Bezeichnung: Verfahren und Kommunikationsvorrichtung zum elektronischen Signieren einer Nachricht in einem Mobilfunktelefon

IPC: H 04 L, H 04 Q

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 22. April 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hoiß

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum elektronischen Signieren einer Nachricht in einem Mobilfunktelefon sowie ein Kommunikationssystem, welches insbesondere zur Durchführung des Verfahrens ausgebildet ist.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren sowie ein Kommunikationssystem zum elektronischen Signieren einer Nachricht bereitzustellen, bei dem ein Personalcomputer unmittelbar über ein Kommunikationsnetz mit einem Mobilfunktelefon, welches als Signiergerät fungieren kann, kommunizieren kann.

Gemäß dem Verfahren wird zunächst ein elektronischer Fingerabdruck aus der zu signierenden Nachricht in einem Personalcomputer (10) erstellt. Der elektronische Fingerabdruck wird vom Personalcomputer (10) über ein Kommunikationsnetz (110) zu einem auswählbaren Mobilfunktelefon (60), welches eine Signiereinrichtung (90) enthält, gesendet. Der empfangene elektronische Fingerabdruck wird im Mobilfunktelefon (60) signiert und zum Personalcomputer (10) zurück gesendet.

Verfahren und Kommunikationsvorrichtung zum elektronischen Signieren einer Nachricht in einem Mobilfunktelefon

Die Erfindung betrifft ein Verfahren zum elektronischen Signieren einer Nachricht in einem Mobilfunktelefon sowie ein Kommunikationssystem, welches insbesondere zur Durchführung des Verfahrens ausgebildet ist.

Die Übertragung von Dokumenten, wie z.B. Antragsformulare und dergleichen, auf elektronischem Wege nehmen in jüngster Zeit rasch zu. Um die Unversehrtheit der übertragenen Daten und die Identität des Urhebers des Dokumentes prüfen zu können, sind Methoden zum digitalen Signieren von Nachrichten entwickelt worden.

Ein solches Verfahren ist beispielsweise aus der DE 197 47 603 T2 bekannt. Bei diesem Verfahren wird eine zu signierende Nachricht von einem Personalcomputer über ein Kommunikationsnetzwerk zunächst an eine vom Personalcomputer getrennt angeordnete Empfangsvorrichtung gesendet. Diese Nachricht wird anschließend von der Empfangsvorrichtung über ein Telefonnetz an ein der Sendevorrichtung zugeordnetes Mobilfunktelefon übertragen, welches als Signiergerät ausgebildet ist. Die Nachricht wird im Mobilfunktelefon auf Anweisung des Nutzers signiert und dann an die Empfangsvorrichtung oder einen anderen Empfänger zurück übertragen. Das bekannte Verfahren weist zwar den Vorteil auf, dass zu signierende Nachrichten von einem Personalcomputer zu einem als Signiergerät fungierenden Mobilfunktelefon übertragen werden können, ohne dass am Personalcomputer selbst Installationen oder andere

Veränderungen vorgenommen werden müssen. Um dies zu erreichen, muss jedoch eine vom Personalcomputer getrennte Empfangsvorrichtung bereitgestellt werden, die die zu signierende Nachricht zum Mobilfunktelefon überträgt und die signierte Nachricht vom Mobilfunkgerät auch wieder empfangen kann.

Ein ähnliches Verfahren ist ferner der EP 1 027 784 zu entnehmen.

Der Erfindung liegt somit die Aufgabe zugrunde, ein Verfahren sowie ein Kommunikationssystem zum elektronischen Signieren einer Nachricht bereitzustellen, bei dem ein Personalcomputer unmittelbar über ein Kommunikationsnetz mit einem Mobilfunktelefon als Signiergerät kommunizieren kann.

Diese Aufgabe löst die Erfindung zum einen mit den Verfahrensschritten des Anspruchs 1.

Danach ist ein Verfahren zum elektronischen Signieren einer Nachricht in einem Mobilfunktelefon vorgesehen. Zunächst wird von der zu signierenden Nachricht in einem Personalcomputer ein elektronischer Fingerabdruck erstellt, der anschließend über ein Kommunikationsnetz zu einem auswählbaren Mobilfunktelefon, welches eine Signiereinrichtung enthält, übertragen wird. Der Personalcomputer kann beispielsweise über einen Internetzugang mit dem Kommunikationsnetz verbunden sein. Der empfangene elektronische Fingerabdruck wird im Mobilfunktelefon signiert und anschließend zum Personalcomputer zurück übertragen.

Vorteilhafte Weiterbildungen sind Gegenstand der Unteransprüche.

Zweckmäßigerweise ist zur Übertragung des elektronischen Fingerabdrucks im Personalcomputer eine Software implementiert, die eine Übertragung des elektronischen Fingerabdrucks über einen SMS (Short Message Service)-, E-Mail- oder WAP (Wireless Application Protocol)-Dienst ermöglicht.

Das elektronische Signieren kann mit Hilfe eines beliebigen kryptographischen Verfahrens, wie zum Beispiel dem Public-Key-Verfahren durchgeführt werden. Hierzu wird zunächst im Mobilfunktelefon ein geheimer Schlüssel, der nicht kopierbar ist, sowie im Personalcomputer ein dem Geheimschlüssel zugeordneter öffentlicher Schlüssel abgelegt. Bei dem öffentlichen Schlüssel kann es sich um einen kryptographischen Schlüssel handeln, der dem Besitzer des Mobilfunktelefons zugewiesen ist. Mit Hilfe des geheimen Schlüssels signiert das Mobilfunktelefon den elektronischen Fingerabdruck und sendet diesen zum Personalcomputer zurück. Der Personalcomputer wiederum wandelt den signierten elektronischen Fingerabdruck mit Hilfe des öffentlichen Schlüssels in einen unverschlüsselten elektronischen Fingerabdruck um. Um festzustellen, ob der übertragene elektronische Fingerabdruck auf den ungeschützten Übertragungswegen des Kommunikationsnetzes nicht manipuliert worden ist, wird der in einen unverschlüsselten elektronischen Fingerabdruck umgewandelte signierte elektronische Fingerabdruck mit dem aus der zu signierenden Nachricht erstellten elektronischen Fingerabdruck verglichen. Stimmen beide elektronische Fingerabdrücke überein, ist sichergestellt, dass keine Manipulation auf den ungeschützten Übertragungswegen zwischen dem Personalcomputer und dem Mobilfunktelefon stattgefunden hat.

Vorzugsweise wird der elektronische Fingerabdruck gemäß einer an sich bekannten Hash-Funktionen aus der zu signierenden Nachricht gebildet und stellt somit einen bestimmten Hash-Wert dar.

Die oben genannte Aufgabe wird ebenfalls durch die Merkmale des Anspruchs 5 gelöst.

Danach ist ein Kommunikationssystem umschrieben, welches wenigstens einen an ein Kommunikationsnetz anschließbaren Personalcomputer und wenigstens ein dem Kommunikationsnetz zugeordnetes Mobilfunktelefon aufweist. Der Personalcomputer enthält eine Einrichtung zum Erstellen eines elektronischen Fingerabdrucks aus einer zu signierenden Nachricht sowie eine Sendeeinrichtung zum Übertragen des elektronischen Fingerabdrucks zu einem auswählbaren Mobilfunktelefon. Das Mobilfunktelefon weist eine Empfangseinrichtung zum Empfangen eines vom Personalcomputer über das Kommunikationsnetz übertragenen elektronischen Fingerabdrucks, eine Signiereinrichtung zum Signieren des empfangenen elektronischen Fingerabdrucks sowie eine Sendeeinrichtung zum Zurückübertragen des signierten elektronischen Fingerabdrucks zum Personalcomputer auf.

Vorteilhafte Weiterbildungen sind Gegenstand der Unteransprüche.

So weist beispielsweise das Mobilfunktelefon einen Speicher zum Ablegen eines geheimen Schlüssels und der Personalcomputer einen ersten Speicher zum Ablegen eines dem geheimen Schlüssel zugeordneten öffentlichen Schlüssels auf. Auf diese Weise ist es möglich, das Signieren einer Nachricht unter Anwendung eines Public-Key-Verfahrens durchzuführen. Der Personalcomputer weist ferner eine Einrichtung zum Umwandeln eines empfangenen signierten elektronischen

Fingerabdrucks mit Hilfe des öffentlichen Schlüssels sowie eine Vergleichseinrichtung zum Vergleichen des umgewandelten elektronischen Fingerabdrucks mit dem aus der zu signierenden Nachricht erstellten elektronischen Fingerabdruck auf.

Um die zu signierende Nachricht, besser gesagt, den aus der zu signierenden Nachricht erstellten elektronischen Fingerabdruck vom Personalcomputer zum Mobilfunktelefon übertragen zu können und von diesem wieder empfangen zu können, ist in dem Personalcomputer eine spezielle Kommunikationssoftware zu implementieren, welche in einem weiteren Speicher abgelegt sei kann.

In einer zweckmäßigen Weiterbildung weist der Personalcomputer einen dritten Speicher auf, in dem wenigstens die Rufnummer des Mobilfunktelefons abgelegt ist, die der Personalcomputer automatisch wählt, wenn eine zu signierende Nachricht von einem Mobilfunktelefon zu signieren ist. Die Rufnummern weiterer Mobilfunktelefone oder anderer über das Kommunikationsnetz erreichbarer Signiergeräte sowie die Rufnummer oder Rufnummern bestimmter Zieleinrichtungen können ebenfalls im dritten Speicher abgelegt werden.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels in Verbindung mit einer Zeichnung näher erläutert.

Die einzige Figur zeigt einen Personalcomputer 10, welcher über ein Kommunikationsnetz 110, beispielsweise ein Mobilfunknetz, mit einem Mobilfunktelefon, kurz auch Handy 60 genannt, verbunden werden kann. Mit Hilfe des beispielhaften Kommunikationssystems kann ein am Personalcomputer 10 erstelltes Dokument signiert und an einen Adressaten, nachfolgend auch Zieleinrichtung 100 genannt, über das Kommunikationsnetz 110 versendet werden.

Hierzu weist der Personalcomputer 10 eine an sich bekannte Sende-/Empfangseinrichtung 20 auf, über die der Personalcomputer 10 mit dem Kommunikationsnetz 110 verbunden ist. In einem Speicher 30 können ein oder mehrere Rufnummern abgelegt sein, die im vorliegenden Beispiel einmal zu dem Handy 60 und zu der Zieleinrichtung 100 gehören, an die ein signiertes Dokument verschickt werden soll. Um, wie weiter unten noch näher ausgeführt, ein Dokument beispielsweise gemäß dem Public-Key-Verfahren signieren bzw. verschlüsseln zu können, ist in einem weiteren Speicher 32 ein sogenannter öffentlicher Schlüssel ablegbar, der dem Besitzer des Handy's 60 gehört und öffentlich zur Verfügung steht. Ein zu signierendes Dokument, welches am Personalcomputer 10 erstellt worden ist, kann in einem Speicher 34 abgelegt werden. Üblicherweise wird jedoch nicht das fertiggestellte Dokument sondern nur ein aus dem fertiggestellten Dokument erstellter elektronischer Fingerabdruck signiert. Ein solcher elektronischer Fingerabdruck kann beispielsweise mit Hilfe einer Hash-Funktion aus dem fertiggestellten Dokument berechnet werden. Der berechnete Wert, auch Hash-Wert genannt, kann in einem Speicher 36 abgelegt werden. Damit der Personalcomputer 10 über das Kommunikationsnetz 110 mit dem Handy 60 kommunizieren kann, ist in einem Speicher 38 eine geeignete Kommunikationssoftware abgelegt. Die Steuerung des Personalcomputers 10, die Berechnung eines elektronischen Fingerabdrucks aus einem fertiggestellten Dokument und die Entschlüsselung eines vom Handy 60 signierten elektronischen Fingerabdrucks kann in dezentralen Einrichtungen oder in einer, wie in der Figur gezeigt, zentralen Steuereinheit 40 erfolgen. Die Steuereinheit 40 ist mit den Speichern 30, 32, 34, 36 und 38 sowie der Sende-/Empfangseinrichtung 20 verbunden.

Das mit einer Signierfunktion ausgestattete Handy 60 weist neben einer an sich bekannten Sende-/Empfangseinrichtung 70 und einer Antenne 120 eine Signiereinrichtung 90 auf, die mit einem Speicher 80 verbunden ist, in dem ein geheimer Schlüssel, insbesondere der geheime Schlüssel des Besitzers des Handy's 60 abgelegt ist.

Nachfolgend wird die Funktionsweise des in der Figur gezeigten Kommunikationssystems näher erläutert.

Angenommen sei, dass ein am Personalcomputer 10 erstelltes Dokument, beispielsweise ein Kaufvertrag in signierter Form zur Zieleinrichtung 100 übertragen werden soll. Das im Dokumentenspeicher 34 zuvor abgelegte Dokument wird von der Steuereinheit 40 ausgelesen. Die Steuereinheit 40 erstellt dann mit Hilfe einer Hash-Funktion aus dem Dokument einen elektronischen Fingerabdruck, der als Hash-Wert bezeichnet werden kann. Dieser Hash-Wert wird im Speicher 36 abgelegt. Über eine Tastatur des Personalcomputers 10 kann nunmehr der Benutzer den Prozess zur Signierung des bestellten Dokumentes einleiten. Hierzu wird entweder automatisch über das Kommunikationsnetz 110 ein Verbindungsaufbau zum Handy 60 eingeleitet, indem die im Speicher 30 hinterlegte Rufnummer des Handys 60 ausgelesen und dem Kommunikationsnetz 110 zur entsprechenden Auswertung zugeführt wird. Sofern es mehrere signierungsfähige Handy's gibt, kann der Benutzer auch selbst die Rufnummer über die Tastatur des Personalcomputers 10 des entsprechenden Handy's eingeben. Anschließend wird der im Speicher 36 abgelegte Hash-Wert über die Sende-/Empfangseinrichtung 20 des Personalcomputers 10 über das Kommunikationsnetz zum Handy 60 übertragen. An dieser Stelle sei angemerkt, dass die Übertragungswege über das Kommunikationsnetz 110 ungeschützt sind. Über die Sende-/Empfangseinrichtung 70 des Handy's 60 gelangt der empfangene Hash-Wert in die Signiereinrichtung 90. Die

Signiereinrichtung 90 und der Speicher 80 können fest im Handy implementiert oder Bestandteil einer Mobilfunkkarte, die in das Handy einsetzbar ist, sein. Zum Signieren des empfangenen Hash-Wertes liest die Signiereinrichtung 90 den geheimen Schlüssel aus dem Speicher 80 aus und verschlüsselt bzw. signiert den Hash-Wert gemäß dem Public-Key-Verfahren. Der signierte Hash-Wert wird anschließend wieder über die Sende-/Empfangseinrichtung 70 und die schematisch in der Figur dargestellte Antenne 120 über das Kommunikationsnetz 110 unmittelbar zum Personalcomputer 10 zurückgesendet. Über die Sende-/Empfangseinrichtung 20 gelangt der signierte Hash-Wert in die Steuereinheit 40, die mit Hilfe des im Speicher 32 abgelegten öffentlichen Schlüssels den signierten Hashwert entschlüsselt, d.h. wieder in den unverschlüsselten Hash-Wert zurückwandelt. Der entschlüsselte Hash-Wert wird dann zusammen mit dem im Speicher 36 hinterlegten, aus dem fertiggestellten Dokument unmittelbar erstellten Hash-Wert der Vergleichseinrichtung 50 zugeführt und darin verglichen. Stimmen der im Speicher 36 hinterlegte Hash-Wert und der entschlüsselte Hash-Wert überein, hat keine Manipulation auf den ungeschützten Übertragungswegen des Kommunikationsnetzes 110 zwischen dem Personalcomputer 10 und dem Handy 60 stattgefunden. Das im Speicher 34 hinterlegte Dokument gilt somit zusammen mit dem im Speicher 36 abgelegten Hash-Wert als signiert; es kann nunmehr zum Adressaten 100 übertragen werden.

Ein gesonderter Wählautomat oder die Steuereinheit 40 liest hierzu die entsprechende Rufnummer (oder eMail-Adresse usw.) der Zieleinrichtung 100 aus dem Speicher 30 aus und leitet, sofern der Adressat am Kommunikationsnetz 110 angeschlossen ist, hierüber einen Verbindungaufbau dorthin auf. Schließlich wird das signierte Dokument zur Zieleinrichtung 100 übertragen

Bezugszeichenliste

10	Personalcomputer
20	Sende-/Empfangseinrichtung des Personalcomputers
30	Speicher für wenigstens eine Handy-Rufnummer
32	Speicher für einen öffentlichen Schlüssel
34	Speicher für ein zu signierendes Dokument
36	Speicher für einen Hash-Wert
38	Speicher für eine Kommunikationssoftware
40	Steuereinheit
50	Vergleichseinrichtung
60	Handy
70	Sende-/Empfangseinrichtung
80	Speicher für einen geheimen Schlüssel
90	Signiereinrichtung
100	Zieleinrichtung
110	Kommunikationsnetz, insbesondere Mobilfunknetz

Patentansprüche

1. Verfahren zum elektronischen Signieren einer Nachricht in einem Mobilfunktelefon (60) mit folgenden Verfahrensschritten:
Erstellen eines elektronischen Fingerabdrucks aus der zu signierenden Nachricht in einem Personalcomputer (10);
Senden des elektronischen Fingerabdrucks vom Personalcomputer (10) über ein Kommunikationsnetz (110) zu einem auswählbaren Mobilfunktelefon (60), welches eine Signiereinrichtung enthält;
Signieren des empfangenen elektronischen Fingerabdrucks im Mobilfunktelefon (60) und
Zurückübertragen des signierten elektronischen Fingerabdrucks zum Personalcomputer (10).

2. Verfahren zum elektronischen Signieren nach Anspruch 1, dadurch gekennzeichnet, dass
im Mobilfunktelefon (60) ein geheimer Schlüssel und im Personalcomputer (10) ein dem geheimen Schlüssel zugeordneter öffentlicher Schlüssel abgelegt werden kann, dass
im Mobilfunktelefon (60) der elektronische Fingerabdruck mit dem geheimen Schlüssel signiert und zurück zum Personalcomputer (10) übertragen wird, und dass
der signierte elektronische Fingerabdruck mit Hilfe des öffentlichen Schlüssels in einen unverschlüsselten elektronischen Fingerabdruck umgewandelt und dieser mit dem aus der zu signierenden Nachricht erstellten elektronischen Fingerabdruck verglichen wird.

3. Verfahren zum elektronischen Signieren nach Anspruch 1 oder 2,

dadurch gekennzeichnet, dass
der elektronische Fingerabdruck gemäß einer Hash-Funktion aus der zu signierenden Nachricht gebildet wird.

4. Verfahren zum elektronischen Signieren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet, dass
die elektronischen Fingerabdrücke zwischen dem Mobilfunktelefon und dem Personalcomputer mittels eines SMS-, E-Mail- oder WAP-Dienstes übertragen werden.

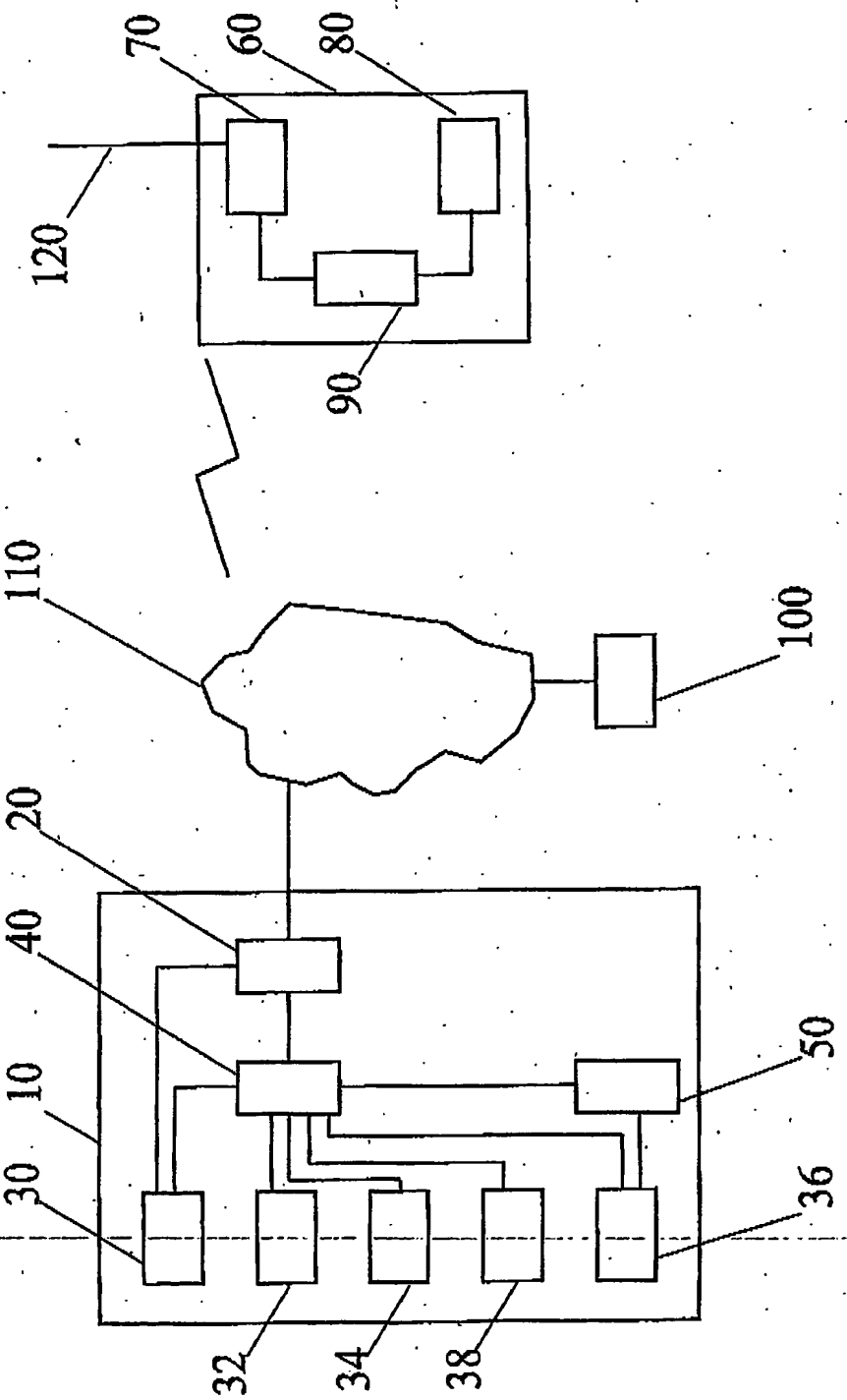
5. Kommunikationssystem, insbesondere zur Durchführung des Verfahrens zum elektronischen Signieren nach einem der Ansprüche 1 bis 4, welches aufweist:
wenigstens einen an ein Kommunikationsnetz (110) anschließbaren Personalcomputer (10) und wenigstens ein dem Kommunikationsnetz zugeordnetes Mobilfunktelefon (60), wobei
der Personalcomputer (10) eine Einrichtung (40) zum Erstellen eines elektronischen Fingerabdrucks aus einer zu signierenden Nachricht und eine Sende-/Empfangseinrichtung (20) zum Übertragen des elektronischen Fingerabdrucks zu einem auswählbaren Mobilfunktelefon (60) enthält, und wobei
das Mobilfunktelefon (60) eine Empfangseinrichtung (70) zum Empfangen eines vom Personalcomputer (10) über das Kommunikationsnetz (110) übertragenen elektronischen Fingerabdrucks, eine Signiereinrichtung (90) zum Signieren des empfangenen elektronischen Fingerabdrucks und eine Sendeeinrichtung (70) zum Rückübertragen des signierten elektronischen Fingerabdrucks zum Personalcomputer (10) aufweist.

6. Kommunikationssystem nach Anspruch 5,
dadurch gekennzeichnet, dass

das Mobilfunktelefon (60) einen Speicher (80) zum Ablegen eines geheimen Schlüssels und der Personalcomputer (10) einen ersten Speicher (32) zum Ablegen eines dem geheimen Schlüssel zugeordneten öffentlichen Schlüssels aufweist, wobei der Personalcomputer (10) ferner eine Einrichtung (40) zum Umwandeln eines empfangenen signierten elektronischen Fingerabdrucks mit Hilfe des öffentlichen Schlüssels sowie eine Vergleichseinrichtung (50) zum Vergleichen des umgewandelten elektronischen Fingerabdrucks mit der aus der zu signierenden Nachricht erstellten elektronischen Fingerabdruck aufweist.

7. Kommunikationssystem nach Anspruch 5 oder 6, dadurch gekennzeichnet, dass der Personalcomputer (10) einen zweiten Speicher (38) zum Ablegen einer Software, die die Kommunikation des Personalcomputer mit dem Mobilfunktelefon (60) ermöglicht, aufweist.

8. Kommunikationssystem nach einem der Ansprüche 5 bis 7, gekennzeichnet durch einen dritten Speicher (30), in dem die Rufnummer wenigstens eines Mobilfunktelefons und/oder einer Zieleinrichtung (100) ablegbar sind und durch eine Einrichtung (40) zum automatischen Anwählen eines Mobilfunktelefons und/oder einer Zieleinrichtung.


70
60
80
120
90
110
100
20
40
10
50
30
36
32
34
38

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☑ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☑ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.